

#ИРО43

ПАМЯТКА

#ЦЦТ43



ИНСТИТУТ РАЗВИТИЯ
ОБРАЗОВАНИЯ
КИРОВОСКОЙ ОБЛАСТИ

БЕЗОПАСНЫЙ ИНТЕРНЕТ

*Правила безопасного пользования
интернетом для детей*



*Сохраняйте себе на страницу
и делитесь с друзьями!*

#ИРО43

ПАМЯТКА

#ЦЦТ43



ИНСТИТУТ РАЗВИТИЯ
ОБРАЗОВАНИЯ
КИРОВОСКОЙ ОБЛАСТИ

1

**ВСЕГДА НУЖНО СОВЕТОВАТЬСЯ
С РОДИТЕЛЯМИ!**

*Перед тем, как зарегистрироваться
на сайте, создать профиль
в социальной сети и выложить
фотографию рекомендуется
посоветоваться с родителями*

#ИРО43

ПАМЯТКА

#ЦЦТ43



2

БЕРЕГИТЕ ЛИЧНЫЕ ДАННЫЕ!



Не нужно рассказывать подробности о себе и о родителях в социальных сетях

#ИРО43

ПАМЯТКА

#ЦЦТ43



ИНСТИТУТ РАЗВИТИЯ
ОБРАЗОВАНИЯ
ОРЛОВСКОЙ ОБЛАСТИ

3

НЕ ДЕЛИТЕСЬ ИНФОРМАЦИЕЙ О СВОИХ ЗНАКОМЫХ!

Не нужно рассказывать про своих друзей и одноклассников, сообщать, где они живут и учатся, какие кружки посещают



#ИРО43

ПАМЯТКА

#ЦЦТ43



4

НЕ ВЕРЬТЕ ВСЕМУ, ЧТО ПИШУТ В ИНТЕРНЕТЕ!

*В интернете
часто можно
найти **фейковую
информацию**,
поэтому не стоит
доверять каждому
информационному
ресурсу*



#ИРО43

ПАМЯТКА

#ЦЦТ43



5

НЕ ОБЩАЙТЕСЬ С НЕЗНАКОМЫМИ ЛЮДЬМИ!

*Назойливость, частые обращения, просьбы
что-то написать и тем более прислать фото
— это повод для того, чтобы сразу же
**прекратить общение и заблокировать
человека***



#ИРО43

ПАМЯТКА

#ЦЦТ43



6 ПОСТАРАЙТЕСЬ ПРИДУМАТЬ СЛОЖНЫЙ ПАРОЛЬ!



Короткий пароль легко запомнить, но его очень просто взломать

Не храните пароли от социальных сетей в информационном пространстве

#ИРО43

ПАМЯТКА

#ЦЦТ43



7 НЕ ИСПОЛЬЗУЙТЕ ОБЩЕСТВЕННЫЙ WiFi

Общественный WiFi часто выручает там, где плохо ловит мобильный интернет.

Но пользоваться им стоит с осторожностью:

многие публичные сети никак не защищены





8

ПОМНИТЕ О ВЕЖЛИВОСТИ!

*В любой ситуации,
даже если кажется,
что это обман,
не стоит грубить
и тем более
использовать
нецензурную лексику*

Как не попасть в руки мошенников?

В век информационных технологий владеть основами безопасности в интернете нужно каждому! О том, как уберечь себя и своих близких от возможных вредоносных действий хакеров, как быстро распознать мошенника, читайте в карточках

КАК БЫСТРО РАСПОЗНАТЬ МОШЕННИКА



5 признаков финансового обмана:

1. Выходят сами

Вам звонит незнакомец, присылает СМС-сообщение, электронное письмо или ссылку в мессенджере

2. Говорят о возможной потере денег или сверхприбыли

Основная задача мошенников — получить доступ к чужим деньгам. Схемы обмана почти всегда связаны с финансами

3. Запрашивают персональные данные

Реальный сотрудник банка не будет просить вас назвать реквизиты или что-то установить на телефон

4. Манипулируют эмоциями

Мошенники стремятся вызвать у вас сильные эмоции — напугать или наоборот, обрадовать новостью

5. Заставляют оперативно принимать решения

Часто мошенники требуют немедленных действий. Если вас торопят с решением, прекратите общение

ТЕЛЕФОННЫЕ МОШЕННИКИ



Приемы:

Представляются сотрудниками банка и пугают потерей средств.
Заводят разговор о переводе денег (оплата штрафов, налогов, услуг).
Заставляют взять кредит.
Просят сообщить реквизиты банковской карты (ее номер, CVV/CVC-код).
Просят продиктовать одноразовый код из SMS.
Просят установить приложение на телефон “для защиты средств”.
Просят срочно перевести деньги на “спасение” близких.

Что делать, если у вас списали деньги:

1. Обратиться в банк и заблокировать счет.
2. Потребовать отменить транзакцию в банке немедленно: некоторые платежи можно успеть вернуть.
3. Потребовать от банка провести чарджбек (оспаривание платежа, с которым вы не согласны). Условия процедуры зависят от политики банка и платежных систем.
4. Обратиться в полицию с заявлением и требованием возбудить уголовное дело.
5. Если в возбуждении дела полиция отказала, можно это оспорить в прокуратуре или суде.

КИБЕРМОШЕННИКИ



Приемы:

Создают подменные сайты, замаскированные под официальные ресурсы компаний (страховая, банк, госучреждение). С помощью них собирают все доступные данные, включая реквизиты карт и счетов (фишинг).

Распространяют вирусное ПО, которое позволяет автоматически переадресовывать вас на поддельные сайты, где похищают данные (фарминг).

Взламывают аккаунты ваших друзей и близких в социальных сетях и мессенджерах, просят “в долг” от их имени.

Представляются несуществующими благотворительными организациями и просят помочь “больным детям”.

Что делать, если у вас списали деньги:

1. Подать заявление в полицию.
2. Если списали деньги без вашего ведома, немедленно обратитесь в банк: заблокируйте счет и постарайтесь оспорить транзакцию.
3. Направьте обращение в департамент по недобросовестным практикам Банка России.